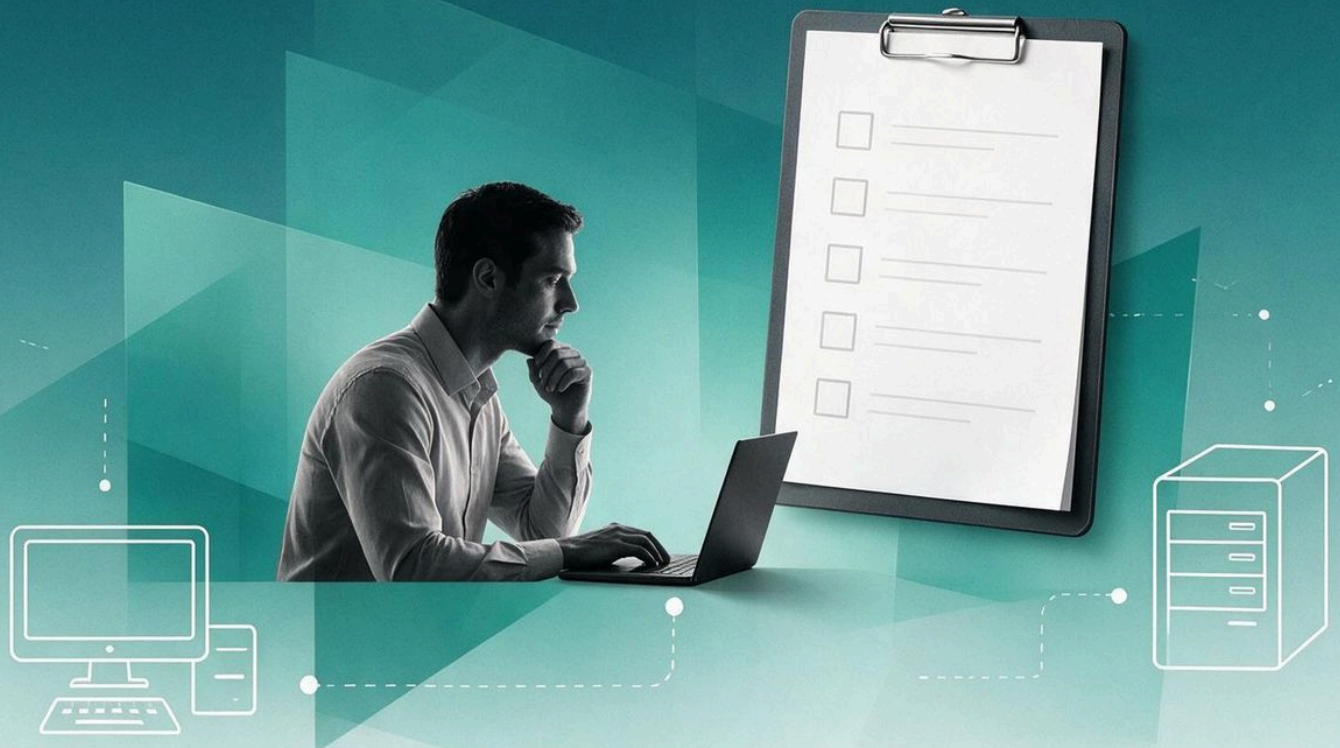




Endpoint Privilege Manager Deployment Checklist



EPM Deployment Checklist

When deploying an endpoint privilege manager, a solution that is deployed on almost all endpoints and servers in an organization, organizations must follow a clear plan of deployment. While it is highly recommended to create a roadmap/rollout plan tailored to the complexities unique to each organization, we recommend the plan is devised along the same lines as the steps discussed in this document.

This deployment checklist document is split into three sections.

1. Pre-deployment Preparation
2. Deployment Phase
3. Post-deployment Validation

Pre-Deployment Preparation

Deploying an endpoint privilege manager is going to change the way users make use of the privileges and permissions. Before you go ahead and roll out the solution for everyone, ensure you have worked on the following:

Business & Security Requirements

Task	Notes
1. Define business objectives for deploying EPM	Whether your goal is to achieve least privilege, demonstrate compliance, eliminate insider threats, progress with zero-trust.
2. Identify the regulations governing your industry	Whether your company is required to be compliant with HIPAA, GDPR, ISO, SOC, PCI-DSS, NERC-CIP

Task	Notes
3. Define policies that govern privileged access	Decide who in your organization should have privileged access, what should be the baseline privileges for users, who should be responsible for enforcing least privilege, and define exceptions for the policy.

Infrastructure Readiness

Task	Notes
1. Check whether your identity provider can be integrated with the EPM solution	Ensure whether the EPM solution can be integrated with Active Directory, Microsoft Entra ID, Google Workspace, or your identity provider.
2. Verify OS compatibility for endpoints	Verify whether the endpoints you want to manage privileges on run on an operating system (Windows, Mac, Linux) compatible with your Endpoint Privilege Manager.
3. Assess network connectivity and firewall rules	Endpoint Privilege Manager works through privilege management agents that are deployed on the endpoints. The agents and the EPM server must be able to communicate frequently for a seamless experience. The firewall rules and network connectivity settings must facilitate communication between the agent and the server.

Task	Notes
4. Create strategies for high-availability and disaster recovery	Endpoint Privilege Managers help users perform their daily tasks and are therefore considered critical for the productivity of the workforce. Configuring a high-availability setup ensures the right privileges are available to the users at the right time. Ensure that a robust high-availability strategy is developed, and the infrastructure is available to make use of the strategy.

Stakeholder Planning

Task	Notes
1. Identify stakeholders (IT, InfoSec, Compliance, Helpdesk).	The Endpoint Privilege Manager is used by the IT helpdesk, cybersecurity teams, and the compliance team to ensure only the minimum required privileges are being granted just at the right time. Ensure everyone who will be impacted by the solution directly, and indirectly. Once identified, list how each of them is going to be impacted.

Task	Notes
2. Define pilot user groups and rollout phases.	When deploying the solution, always rollout in phases. Identify the pilot group and let them know in advance about the changes being made to their workflow. When rolling out, follow this procedure: 1. Deploy Securden Agent 2. Run Agent in Learning Mode. 3. Create Policy Using Insights Gathered by the Agent. 4. Remove Admin Rights. These will be explained further in the 'Deployment Phase' section of this document.
3. Communicate policy changes to end-users.	Once the test run with the pilot group is successful, communicate the policy changes to the end-user before extending the roll out to everyone.

Backup & Rollback

Task	Notes
1. Backup critical configurations (AD, system images).	Ensure you have taken a backup of all critical configurations in your Active Directory, Entra ID, and Google Workspace domain. Ensure you have taken a backup of all data on the device on which Securden Endpoint Privilege Manager is going to be installed.
2. Create Rollback points if the deployment fails.	Create a rollback point on the device that is going to act as the Endpoint Privilege Manager server. If the installation fails due to unforeseen circumstances, you can easily revert to a safe rollback point and try again.

Deployment Phase

The deployment phase of Securden Endpoint Privilege Manager involves onboarding users and computers, deploying Securden agents on endpoints, creating control policies to automate privilege elevation, and removing admin rights from endpoints. Ensure you follow the checklist below.

Backend Database Server

Task	Notes
1. Between PostgreSQL, and MS SQL, decide which backend database server you wish to make use of for the Endpoint Privilege Manager.	You can make use of the bundled PostgreSQL database when starting out and migrate to MS SQL whenever you want. While both options are supported and highly scalable, deciding early on will eliminate unnecessary migration later.

Mandatory Settings

Task	Notes
1. Encryption Key	When you apply the registered license key, you will be prompted to move the installation encryption key to a location other than the installation folder. This is to ensure that the encrypted data and the encryption key are not kept together. Follow the instructions on the interface to complete this step.
2. Mail Server Settings	Securden Endpoint Privilege Manager sends various emails to users and admins. To facilitate this, the mail server settings must be configured. You can choose between using OAuth or basic authentication for this purpose. If you choose to proceed with OAuth, Securden readily integrates with Outlook and Gmail. Navigate to Admin >> General >> Mail Server Settings to configure this.

Task	Notes
3. Proxy Server Settings	If your organization makes use of a proxy server to regulate internet traffic, configure the proxy server for details here to facilitate Securden to connect to the internet. Navigate to Admin >> General >> Proxy Server Settings in the GUI to perform this step. Internet connectivity is required if you want to use the Secure Remote Assist capability.
4. Server Connectivity Settings	This setting is to specify how the Agents connect to the Securden web interface from endpoints and the name with which the client machines identify the Securden server host. Navigate to Admin >> General >> Securden Server Connectivity in the GUI to perform this step.

Computer Onboarding and Management

Task	Notes
1. Integration with Directories	You can integrate with Active Directory, Entra ID, and Google Workspace for onboarding your computers and computer groups. You can keep the groups in Securden in continuous synchronization with your directories.

Task	Notes
2. Deploying the Securden Agent	You can deploy the Securden Agent on endpoints through one of the following methods. 1. Direct installation 2. GPO, SCCM 3. Intune, PDQ Once installed, the Securden Agent will automatically fetch the device details and display that on your Computers tab.
3. Agent Mode	Set the agent mode to 'Learning' by navigating to Computers >> Actions >> Switch Agent Mode. The agent would observe user behavior and provide insights for streamlined policy creation.
4. Assigning Device Owners	Go to Admin >> Configurations and set the option named Discovery of Device Owners to Discover Device Owners. You can exercise options that grants automatic approval to requests raised by device owners to reduce IT helpdesk burden.

User Onboarding and Management

After the agent has been deployed into endpoints, the agents will fetch the local user accounts from the endpoints automatically. You can add domain users or add native users for accessing the EPM web interface.

Task	Notes
1. Onboarding Domain Users	Once you have integrated with Active Directory or Microsoft Entra ID, you can onboard them into Securden by navigating to Users >> Add .
2. Assigning Roles to Users	Onboarded users must have clearly demarcated responsibilities and associated permissions within the Endpoint Privilege Manager. You can assign roles from Users >> Actions >> Change Role. You can choose from the default roles or create custom roles with specific powers. Go to Admin >> Custom User Role to create new user roles.
3. Delete the default Securden Administrator account	By default, the EPM comes with a built-in administrator account. You may replace that account with a locally created administrator account of your own. Use this account to serve emergency access scenarios.

Task	Notes
4. Enforce Two-factor Authentication	You can enforce two-factor authentication for users to login to the Securden interface and for elevating privileges. You can configure 2FA by navigating to Admin >> Two Factor Authentication. You can navigate to Admin >> Configurations and enforce MFA for elevating privileges.
5. Configure SSO	You can integrate with SAML compliant solutions to provide SSO experience to users when they try to login to Securden. Navigate to Admin >> SAML SSO to configure single-sign-on.

Privilege Management and Application Control

Task	Notes
1. Application Repository	Once the Securden agent is installed on endpoints, the agent will observe the apps being run with admin rights and import them into Securden. You can find the list of apps discovered by the agent along with a set of built-in apps in the Applications Tab. You can manually add apps by defining attributes like file name, publisher details, file path, or a combination of attributes. These attributes are used by the agent to identify the application during privilege elevation. So, it is recommended to be very accurate when defining them.
2. Policies for Privilege Elevation	You can create policies that allow specific users to elevate specific apps automatically. Ensure that you create policies to address all routine requirements of all teams to avoid a pile of requests and helpdesk tickets requesting admin rights. You can explore the built-in policies that grant teams the permission to elevate apps they would need the permission to run as admin.

Task	Notes
3. Approval Workflow for On Demand Privileges	You can enforce multiple levels of approval for gaining privileges. Ensure you designate specific approvers for teams to delegate the responsibility and reduce helpdesk burden.
4. Application Control	You can create application allowlists and blocklists to control which applications users and user groups can run. These policies don't grant admin privileges to users, even for specific apps. The apps will run with the same privileges as the user.
5. Automatic Approval Policies	You can configure automatic approvals for requests raised by certain users/groups or for device owners alone. You can use these policies for developers and similar users who need to install and run apps/scripts with admin rights to accomplish their tasks and fulfill their duties.
6. Technician Access Policies	Ensure you have created policies for your technicians to help them provide troubleshooting and technician support securely without using admin account credentials. Allow technicians to sign up using standard user accounts and elevate specific applications/files when required using the Securden Agent.

Integrations

Task	Notes
1. Ticketing System and ITSM	Securden tightly integrates with ITSM solutions to support approval/rejection of requests directly from the Ticketing System. Navigate to Admin >> Integrations >> Ticketing Systems and ITSM to configure this.
2. SIEM for Centralized Monitoring	You can integrate Securden with SIEM solutions and send syslog data for centralized monitoring. Navigate to Admin >> Integrations >> Syslog for SIEM to configure this.

Miscellaneous

Task	Notes
1. Notifications	You can enable alerts for specific Windows events by navigating to Admin >> Notify Windows Events and check all the events you want to trigger alerts upon occurrence. For example, you can configure alerts when a new admin account is created on endpoints during temporary admin access. Similarly, you can configure alerts for events within the Securden interface. You can explore this further using the options available under Admin >> Notifications.
2. Redundancy Measures	You can configure periodic backups of the Securden database and configure high availability servers from Admin >> High Availability to ensure that least privilege is enforced even in unforeseen circumstances.
3. API Access to Securden	You can make use of API tokens for programmatic access to the Endpoint Privilege Manager. You can use these APIs to fetch and manage active requests, manage applications, manage policies, and much more.

Task	Notes
4. Customizing the Web Interface	You can change the language of the web interface, switch the Securden logo with your own, customize email templates, choose the theme of the interface among other options. You can explore these from Admin >> Customization.

Post Deployment Validation

Task	Notes
1. Testing Policies	Once you have created a control policy for a user/user group, test whether the policy has taken effect. In the endpoint, open the Agent tray icon, and pull the latest changes from the server. Try running the app (in the policy) by right-clicking and selecting 'Run with Securden Privilege'. The app should run with admin rights. If it doesn't try reconfiguring. If issue persists, contact support@securden.com

Task	Notes
2. Testing Approval Workflow	Once admin rights are removed, try running an app with admin rights using a standard user account. You should be able to raise a request by specifying the time parameters. Once raised, log in to the web interface as the Securden administrator. Go to Admin >> Privilege Elevation Requests. You should be able to Approve or Reject the request from here. Test both cases at the endpoint.
3. Creating Policies from Requests	Raise a request from an endpoint. Open the requests page in the web interface and click Approve. In this window, you will be able to see a checkbox named Create a Control Policy. Then create a new policy or add it to an existing policy. Then test privilege elevation on any endpoint associated with the created policy.

Task	Notes
4. Testing Notifications	If you have configured Event Notifications, Windows Event Notifications, or Email Notifications, simulate the scenario and verify you are receiving the alert promptly. If you are not receiving alerts, ensure the mail server settings are configured properly and verify the recipient's email address. If issue persists, reach out to support@securden.com
5. Monitoring Product Upgrades	You can look out for the latest releases of Securden Endpoint Privilege Manager from www.securden.com/endpoint-privilege-manager/release-notes.html